Power Wealth Management LLC

Registered Investment Adviser (RIA) Privacy Policy

Version 04.2023

Power Wealth Management LLC
302 Bombay Lane
Roswell, GA 30076
Phone: (404) 889-8919
Fax: (678) 999-4254

19. PRIVACY POLICY

The Firm views protecting its clients' private information as a top priority has instituted the following policies and procedures to ensure that client information is kept private and secure.

19.1 Privacy Policy

Neither the Firm nor any of its Supervised Persons may share nonpublic personal information of consumers or clients with nonaffiliated third parties, except as required to provide the services offered or as otherwise disclosed in the Firm's privacy notice. Supervised Persons are strictly prohibited from taking client information when they leave the Firm. Client information and accounts belong to the Firm.

19.2 Scope of Policy

The Firm's privacy policies and procedures cover the practices of the Firm and apply to all nonpublic personally identifiable information of current and former clients.

19.2.1 Application of Policy to Former Clients

If a client decides to close his or her account with the Firm or becomes an inactive client, the Firm and its Supervised Persons are still required to adhere to the privacy policies and procedures with respect to that client.

19.2.2 Honoring Opt-Out Requests

The Firm and its Supervised Persons must honor any opt-out requests or notices received from consumers or clients.

19.3 Privacy Notices

New clients must receive an initial privacy notice and annual privacy notices thereafter. A notice or revised privacy policy must be delivered to consumers and clients if the Firm seeks to disclose nonpublic personal information in a way that is not accurately described in its previously delivered notices. The Designated Supervisor is responsible for disclosing any changes to its privacy policy 30-days prior to its privacy policy prior to implementation. Additionally, the Designated Supervisor is responsible for providing appropriate opt out elections by the covered consumers and/or clients.

19.3.1 Initial Privacy Notice

Advisors are responsible for delivering the initial privacy notice to a client no later than the time a client relationship is established. This delivery obligation applies even when there is no intent to disclose nonpublic personal information about the client.

19.3.2 Annual Privacy Notice

The Firm will arrange for delivery of annual privacy notices to clients. Annual notices must be provided at least once during any period of twelve consecutive months during the continuation of a client relationship.

A notice or revised privacy policy must be delivered to consumers and clients if the Firm seeks to disclose nonpublic personal information in a way that is not accurately described in its previously delivered notices. The Designated Supervisor is responsible for arranging the delivery of any revised privacy notice at least 30 days prior to the change of policy. If the Firm intends to share client information with nonaffiliated third parties, the privacy notice must include a reasonable means for the client to opt out.

19.3.3 Revised Privacy Notices

A notice or revised privacy policy must be delivered to consumers and clients if the Firm seeks to disclose nonpublic personal information in a way that is not accurately described in its previously delivered notices. The Designated Supervisor is responsible for arranging the delivery of any revised privacy notice at least 30 days prior to the change of policy. If the Firm intends to share client information with nonaffiliated third parties, the privacy notice must include a reasonable means for the client to opt out.

19.4 Safeguarding of Client Information

Supervised Persons play a pivotal role in safeguarding client information.

19.4.1 Limiting Access to Client Information

Access to client information should be limited to persons with a legitimate business need for the information, such as persons who need access to a client's information in order to service the client's account. Supervised Persons are responsible for ensuring that security controls are adequate to prevent unauthorized persons from accessing information.

19.4.2 Securing Client Information

Hard copy documents should be secured by locking the file cabinet or office in which they are stored. Client information kept on the Firm's computers must be password-protected and secured behind firewalls.

19.4.3 Proper Disposal of Client Information

Supervised Persons must use a paper shredder for the destruction of all client-related documents that are not required to be retained by the Firm. With prior approval of the Firm, Supervised Person may use a reputable provider of document shredding services.

19.4.4 Adhering to Information Security Policies and Procedures

The Firm has established information security policies and procedures (described below). These policies and procedures are designed to protect not only the Firm's proprietary information but also the nonpublic information about its clients. Accordingly, adherence to the Firm's privacy policies and procedures also entails adherence to all of the Firm's policies and procedures governing information security.

19.4.5 Preventing the Unauthorized Sharing of Client Information by Departing Supervised Persons

A Supervised Person departing from the Firm may not take client information to his or her new employer without authorization. The transfer of client information to or from the Firm requires pre-approval. Prior to authorizing the sharing of client information, the Designated Supervisor will verify that the sharing of such information is permissible under the circumstances. No sharing of client information may occur until the Designated Supervisor has given formal approval.

Supervised Persons who resign or are otherwise terminated are prohibited from taking any client information from the Firm. The Firm will report the theft of client information to the appropriate authorities.

19.4.6 Preventing the Unauthorized Sharing of Client Information by New Hires

A newly hired Supervised Person may not take client information from his or her prior firm without proper authorization. Similarly, a Supervised Person departing from the Firm may not take client information to his or her new firm without authorization.

19.5 Reporting Privacy Violations

If at any time a Supervised Person suspects the misuse or mishandling of client information or identity theft, he must immediately notify the Designated Supervisor. As required or deemed appropriate, the Designated Supervisor will promptly report any suspected identity theft to the SEC and Federal Trade Commission and retain copies for the files. Supervised Persons are responsible for honoring any opt-out requests received from clients or consumers.